International Journal of Current Research and Review
DOI: 10.7324/IJCRR.2017.9227

Research Article

IJCRR
Section: Technology
Sci. Journal
Impact Factor
4.016
ICV: 71.54

Comparative Analysis of Different Modified Advanced Encryption Standard Algorithms over Conventional Advanced Encryption Standard Algorithm

Kirti Prakash Choudhury[1], Sangeeta Kakoty[2]

[1]Research Scholar, Department of Computer Science & Engineering, Assam down town University, Assam, India; [2]Associate Professor, Department of Computer Science & Engineering, Assam down town University, Assam, India.

ABSTRACT

During the recent times, with the tremendous growth of digital data communication over computer network, information content security becomes a prime concern. Internet itself allows many security threats and those can easily corrupt the transferred data over network. Cryptography plays an important role by providing security for digital transmission of data over such insecure network. Cryptographic protocols scramble data into unreadable text which can be only read or decrypted by those possesses the associated key. The Advanced Encryption Standard (AES) is symmetric key algorithm which provides higher security with higher encryption speed and throughput but still modifications are going on to improve its performance. In this paper we survey and analyze several modifications on AES encryption techniques on different parameters and compare their performance with conventional AES.

Key Words: Cryptography, AES Algorithm, Decryption, Encryption, Block cipher, S-Box, Encoder, Key stream generator, Field Programmable Gate Array

INTRODUCTION

The rapid growth of digital data transmission has significantly increased the importance of information security in our modern digital life. In data communication the development of new transmission technologies have ascended the need of specific strategy for security mechanisms. Network security has become more and more pivotal as digitalization and transmission of large data over internet have been transforming from time to time. Cryptography and different encryption techniques provide security and protection to the data transmitted over non secure networks used for digital transmission of data. The Advanced Encryption Standard (AES) known as Rijndael is a well-known symmetric block cipher algorithm adopted by the United States of America government as a national encryption algorithm and it provides portability, robustness and high level security against many cryptographic attacks. To have better performance, certain efforts have already been made in redesigning and reconstructing the AES algorithm. In this paper we are discussing about different modifications on AES algorithm and comparing their result on the basis of different parameters. To enhance the efficiency of AES, researchers sometimes modified the existing structure of the AES algorithm and sometimes merging the AES block cipher with other models from various fields.

Here in this paper, we try to find out several characteristics of all those modified algorithms so that it will help other researchers to develop an efficient algorithm and which will be implemented in more secured manner. As the comparison is on the basis of the conventional AES algorithm, we are giving a brief overview of this algorithm in the next section.

Corresponding Author:
Kirti Prakash Choudhury, Research Scholar, Department of Computer Science & Engineering, Assam down town University, Assam, India; Contact No.: +91-87219-41305; Email: choudhurykirti@gmail.com

ISSN: 2231-2196 (Print) **ISSN:** 0975-5241 (Online)

Received: 21.09.2017 **Revised:** 15.10.2017 **Accepted:** 10.11.2017

Advanced Encryption Standard Algorithm

The Advanced Encryption Standard is based on the Rijndael cipher developed by Joan Daemen and Vincent Rijmen. It is a symmetric block cipher that processes data blocks of 128 bits using key size of 128, 192, and 256 bits. Each data block of 128 bit data is divided into 16 Bytes. These bytes are mapped to a 4 x 4 array called as the state and all operations of AES are performed on this state [1]. For full encryption, AES uses several rounds (Nr = 10, 12, 14) in which each round is made of four stages. The different four stages found in each round are as follows:

- ByteSub transformation: This is a non linear byte Substitution step in which each byte in the state matrix is replaced with another byte using a Substitution table (S-box), which is constructed by multiplicative inverse and affine transformation.
- ShiftRows transformation: This is a simple byte transformation where the bytes in the first row are not shifted. But second, third and fourth rows are shifted cyclically to the left by one byte, two bytes and three bytes respectively.
- MixColumns transformation: This stage is equivalent to a matrix multiplication of each column of the states. Each column vector is multiplied by a fixed matrix. In this stage bytes are treated as polynomials rather than numbers.[2]
- AddRoundKey transformation: This is a bitwise Exclusive-OR (XOR) operation between the present state and the roundkey. This transformation is its own inverse.[2]

In AES algorithm, encryption procedure starts with an Add Round Key stage followed by (Nr-1) rounds having four stages each and the encryption process ends with the last round which contains three stages. This full encryption and decryption procedure is shown by Figure-1. This diagrammatic representation is cited here for references because most of the modifications done in the AES algorithm is reflected in these step directly or indirectly.

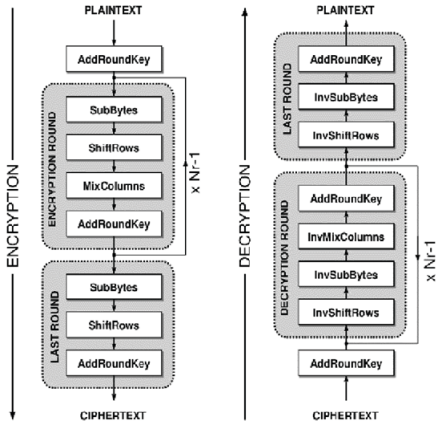

Figure 1: Block Diagram of Main Steps of AES [3] (Source: http://www.iis.ee.ethz.ch/~kgf/acacia/fig/aes.png)

The decryption procedure is the exactly the inverse of encryption procedure consisting also four stages namely InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey.

Conventional AES-128 algorithm provides better security, better encryption speed, and better throughput in comparison to other symmetric encryption technique. But still modifications are going on to reduce hardware resources, increase security against statistical attacks, better encryption speed, less overhead on the data, transferring large scale multimedia data as per different needs in different situations.

Related Work

We all know that conventional AES provides good encryption-decryption speed, and throughput. It has high security than other existing encryption-decryption algorithm. Then also researchers are trying to modify this algorithm to enhance its security, encryption-decryption time and to increase throughput as per requirement. Some of modifications to improve AES are discussed below:

Shtewi *et. al.* presented a concept on modification to the Advanced Encryption Standard (MAES) to reflect a high level security and better image encryption. The modification is done by adjusting the Shift Row phase [2].

Ritu & Vikas proposed a modified AES having 200 bit block as well as key size using 5x5 Matrix unlike the conventional 128 bit AES with 4x4 Matrix. The proposed work is then compared with the 128, 192, 256 bit AES. Only the mix column transformation is changed in this process. The result shows encryption speed and throughput at encryption end is increased and decryption speed, throughput at decryption end is decreased than conventional AES Algorithm [4].

Dandekar *et. al*. proposed a modified symmetric AES algorithm. They used 512 bit length in order to provide a high level of security and high throughput required application. Strength of the AES algorithm is enhanced by increasing the key length to 512 bit and in order to provide a stronger encryption method for secure communication the number of rounds is increased [5].

Vandana C. Koradia is concerned with optimizing the existing standards of cryptography for the images and text data encryption. The modification is done by totalling the Initial Permutation step, takes from Data Encryption Standard (DES), in order to enlarge the encryption performance. This modification indubitably increases the efficiency of encryption and makes the algorithm speedier than the existing one [6].

Manish Kumar Aery has proposed combination of encryption feature of AES and compression feature of Base64 encoder to develop an efficient encryption system that can

encrypt the data and thus saving time and increasing the throughput. First Base64 encoder encodes or converts the text into string value or whole data into string and then encrypted by AES algorithm; finally cipher text is generated. After encoding the size of file is further reduced and is then sent to encryption that further reduces the time for processing [7].

Zeghid *et. al.* proposed a new encryption schemes by adding a key stream generator, such as (A5/1, W7), to the AES algorithm in order to increase the high image security and increase encryption performance, mainly for images characterised by reduced entropy. Key stream generator into AES for image encryption helps to overcome the problem of textured zones and increase encryption performance [8].

Yogeswari & Eswaran proposed an elegant and novel method to enhance security aspects by associating cryptographic techniques along with Steganography. This paper offers confidence and trust by make use of improved dual key AES algorithm along with Steganography [9].

Abdulazeez & Tahir proposed two architectures, one for AES Encryption 128-bit process, and the other for AES Decryption 128-bit process. Both architectures are based on an Iterative structure and modifications such as merging transformation, Look Up tables for decryption, generating keys, and optimization of each clock cycle to incorporate maximum number of operations to improve the throughput and reducing hardware resources [10].

Comparative Analysis

To improve the performance of AES algorithm, numerous efforts have been done in redesigning and reconstructing of AES that we have discussed in the previous section. A comparative analysis of performance of different modified AES algorithms in comparison to conventional AES algorithm is done on the basis of six different parameters, which is discussed below and shown in Table-1.

Performance of all modified AES in terms of Encryption and Decryption speed are better than the conventional AES, except AES-512 algorithm and AES-200 algorithm. In AES-512 algorithm, due to increase in number of round, the encryption and decryption procedures become more complex thereby degrading the speed. Thus there is a tradeoff between speed and security. Again in AES-200 only decryption time per bit slightly decreased but encryption time per bit up to 20% and decryption time per bit increased up to 25% than conventional AES. On the other hand, modification done by Vandana C. Koradia using Initial Permutation table replacing Mix Column step of AES highly increases encryption and decryption speed, which is helpful for multimedia data encryption.

The throughput may be defined as number of bits that can be encrypted or decrypted during one unit of time [4]. From the Table-1, it is observed that out of these eight different modifications on AES, more or less all the modified AES algorithms are performing well in respect of throughput, but AES-512 algorithm and AES with merging transformation show excellent performance by giving about double throughput. Again some modifications failed to show any significant rise of throughput after merging additional technology with the conventional AES.

There are many methods used by researchers in the design and modification of AES block cipher in order to enhance

Table 1: Performence Analysis and Comparison of Various Modified AES Algorithms

Parameters	Key Length (Bits)	Added Technology	Encryption Speed	Decryption Speed	Throughput	Security
AES with adjustment of ShiftRow [2]	128	NO	Increased	Increased	Increased	High
AES-200 [4]	200	NO	Increased	Decreased	Increased	High
AES-512 [5]	512	NO	Decreased	Decreased	Double Increased	Extreme High
AES with Permutation Table [6]	128	NO	Highly Increased	Highly Increased	Increased	Good
AES with Base64 Encoder [7]	128	YES	Increased	Increased	Increased	Extreme High
AES with A5/1 & W7 Encoder [8]	128	YES	Increased	Increased	Good	High
AES with Stagnography [9]	128	YES	Good	Good	Good	Extreme High
AES using FPGA [10]	128	NO	Increased	Increased	Highly Increased	Good

the security of the algorithm and some including merging the AES block cipher with other models from various fields [11]. AES algorithms provide strong security but there are still some issues related to Brute Force attack and Statistical attacks. From Table-1, it is observed that the security strength of modified AES algorithms has improved, but implementation of Permutation Table in AES reduces security strength of AES algorithm. In our study, we analysed that AES-512 algorithm provide extreme high security by increasing key bit length and numbers of rounds. Merging of technology like Stagnography and Encoder like Base64 with AES able to provide higher security than the conventional AES. Also the modified algorithm (MAES) gives better encryption results in terms of security against statistical attacks in comparison to original AES.

CONCLUSION

In this paper we surveyed and analyzed several modifications on AES encryption techniques on different parameters and compared their performance with conventional AES. Performance of these modified AES algorithms vary on different parameters. Generally, with the increase demand of strong security where high level security is needed, we have to compromise with encryption speed in those modifications. Again for encryption of large data like multimedia data, higher encryption speed is needed, for which security is somewhere to be compromised to achieve higher encryption speed. These modifications are useful in different conditions according to the situation demanded. Therefore modifications on AES should focus on designing such methods and techniques that could be used on existing applications in an efficient manner and provide us a highly secured, extremely fast encryption system which can provide high security against all attack including Statistical attack and Brute Force attack and also encrypt large data including multimedia data at very high speed.

ACKNOWLEDGMENT

Authors acknowledge the immense help received from the scholars whose articles are cited and included in references of this manuscript. The authors are also grateful to authors / editors / publishers of all those articles, journals and books from where the literature for this article has been reviewed and discussed. The first author also acknowledges the academic support given by Assam down town University (AdtU), Guwahati, Assam.

REFERENCES

1. Patel, F. R., Dr. Cheeran, A. N. (2015). Performance Evaluation of Steganography and AES encryption based on different formats of the Image. *International Journal of Advanced Research in Computer and Communication Engineering, 4*(5), 659-664, ISSN (Online) 2278-1021 ISSN (Print) 2319-5940, DOI 10.17148/IJARCCE.2015. 45140 664. Retrieved from https://www.ijarcce.com/upload/2015/may-15/IJARCCE%20140.pdf on 27/04/2017 at 11:45 PM.
2. Shtewi, A.A., Hasan, B. E. M., Hegazy, A. El F. A. (2010). An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems. *International Journal of Computer Science and Network Security (IJCSNS), 10*(2), 226-232. http://paper.ijcsns.org/07_book/201002/20100234.pdf on 08/08/2017 at 01:25 AM
3. Gurkaynak, F. K. (2006). *GALS System Design:Side Channel Attack Secure Cryptographic Accelerators.* Retrieved from https://iis-people.ee.ethz.ch/~kgf/ acacia/fig /aes.png on 15/06/2017 at 10:25 PM
4. Pahal, R., Kumar, V. (2013). Efficient Implementation of AES. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(7), 290-295, ISSN: 2277 128X. http://ijarcsse.com/Before_August_2017/docs/papers/Volume_3/ 7_July2013/V3I7-0246.pdf on 27/04/2017 at 11:45 PM.
5. Dandekar, A. K., Pradhan. S., Ghormade. S. (2016). Design of AES-512 Algorithm for Communication Network. *International Research Journal of Engineering and Technology (IRJET),3* (5), 438-443, e-ISSN: 2395 -0056. https://www.irjet.net/archives/V3/i5/IRJET-V3I592.pdf on 27/04/2017 at 12:13 AM
6. Koradia, V. C. (2012-2013). Modification in Advanced Encryption Standard. *Journal of Information, Knowledge, and research in Computer Engineering, 2*(2), 356-358, ISSN: 0975 – 6760. http://www.ejournal.aessangli.in/ASEEJournals/CE73.pdf on 26/05/2017 at 12:33 AM
7. Aery, M. K. (2016). String Compression Technique with Modified AES Encryption. *International Journal of Advanced Computing and Electronics Technology (IJACET),* 3(1), 13-25, ISSN (Print): 2394-3408, (Online): 2394-3416. http://troindia.in/journal/ijacet/vol3iss1/13-25.pdf on 09/06/2017 at 08:37 PM
8. Zeghid, M., Machhout, M., Khriji, L., Baganne, A. and Tourki, R. (2007). A Modified AES Based Algorithm for Image Encryption. *International Journal of Computer, Electrical, Automation, Control and Information Engineering, 1*(3), 745-750, www.waset.org/Publication/7580 on 25/05/2017 at 1.03 AM
9. Yogeswari, G., Eswaran, P. (2016). Enhancing Data Security for Cloud Environment based on AES Algorithm and Steganography Technique. *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), 3*(20), 233-236. http://ijartet.com/v3s20alagappa on 27/04/2017 at 12:52 AM
10. Abdulazeez, A. M., Tahir, A. S. (2013). Design and Implementation of Advanced Encryption Standard Security Algorithm using FPGA. *International Journal of Scientific & Engineering Research, 4*(9), 1988-1993, ISSN 2229-5518. https://www.ijser.org/paper/Design-and-Implementation-of-Advanced-Encryption-Standard-Security-Algorithm-using-FPGA.html on 08/08/2017 at 01:55 AM
11. Juremi, J., Mahmod, R., Zukarnain, Z. A., Yasin, S. Md. (2017). Modified AES S-Box Based on Determinant Matrix Algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering, 7*(1), 110-116, ISSN: 2277 128X. http://ijarcsse.com/Before_August_2017/docs/papers/Volume_7/1_January2017/V7I1-01112.pdf on 08/08/2017 at 01:46 AM